

An analytical proof for Lehmer's totient conjecture using Mertens' theorems

Ahmad Sabihi

Teaching professor and researcher at some universities of Iran

Abstract

We make an analytical proof for Lehmer's totient conjecture. Lehmer conjectured that there is no solution for the congruence equation $n - 1 \equiv 0 \pmod{\phi(n)}$ with composite integers n , where $\phi(n)$ denotes Euler's totient function. He also showed that if the equation has any composite solutions, n must be odd, square-free, and divisible by at least 7 primes. Several people have obtained conditions on values n , and number of square-free primes constructing n if the equation can have composite solutions. Using Mertens' theorems, we show that it is impossible that the equation can have any composite solution and implies that the conjecture should be true for all the positively composite numbers.

Keywords: Lehmer's totient conjecture; Mertens' theorems; Euler's totient function

MSC 2010:11P32;11N05

Email address: sabihi2000@yahoo.com (Ahmad Sabihi)

1. Introduction

Lehmer's totient conjecture was stated by D.H. Lehmer in 1932 [1]. Lehmer conjectured that there are no composite solutions, n , for the equation $n - 1 \equiv 0 \pmod{\phi(n)}$. We know that this conjecture is true for every prime numbers. He also proved that if any such n , exists, it must be odd, square-free, and divisible by at least seven primes [1]. Pinch calls such an n a *Lehmer number* and defines the *Lehmer index* of n to be the ratio $\frac{n-1}{\phi(n)}$ [2]. As we should know every exponent $\lambda(n)$ of the multiplication group $(\mathbb{Z}/\mathbb{N})^*$ must divide $n - 1$ and follows that a Carmichael number n must be square-free with at least three prime factors, and $p - 1 | n - 1$ for every prime p dividing n . Conversely, any such n must be a Carmichael number. Since the exponent $\lambda(n)$ of the multiplicative group divides its order $\phi(n)$, a Lehmer number must be a Carmichael number. Lieuwens [3] showed that a Lehmer number divisible by 3 must have index at least 4 and hence must have at least 212 prime factors and exceeds $5 \cdot 10^{570}$. Kishore [4] proved that a Lehmer number of index at least 3 must have at least 33 prime factors and exceeds $2 \cdot 10^{56}$. Cohen and Hagis [5] showed that a Lehmer number divisible by 5 and of index 2 must have at least 13 prime factors and if we have any composite solution n , to the problem, then $n > 10^{20}$ and number of prime factors must be greater than or equal 14. We firstly show that using Mertens' theorems, we are able to asymptotically prove that the equation $n - m\phi(n) = 1$ with odd composite number n , and having k square-free prime factors cannot have any solutions. We also investigate about the equation $n - m\phi(n) = -1$ and take a conclusion that this equation may have solutions as Lehmer has shown in his paper [1]. We decompose our proof into the four theorems 3 to

6. Then, we show that n , must be odd, and square-free as Lehmer showed before, but by another method. To prove our theorems, we make use of Mertens' theorems on the density of primes and re-prove some of them.

2. Theorems

2.1. Theorem 1: Mertens' 2nd theorem [6]

Let p be a prime and $x > 1$ every real number, then

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + a + O\left(\frac{1}{\log x}\right) \quad (2.1)$$

where a possible value of "a" can be $a = 0.2614972128\dots$

2.2. Theorem 2: Mertens' 3rd theorem [6]

Let p be a prime and $x > 1$ every real number, then

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log x} \quad (2.2)$$

where the notation $f(x) \sim g(x)$ means that limitation $\frac{f(x)}{g(x)} = 1$ when x tends to infinity. γ denotes Euler's constant.

2.3. Corollary 1:

Let p be a prime, $x > 1$ every real number, and $c > 0$ an absolute constant, then

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) > \frac{c}{\log x} \quad (2.3)$$

where "c" can be 0.3 for $x \geq 2973$ and 0.09 for $x \geq 3$ in this paper.

2.4. Theorem 3:

Let p_i to p_k be all of the prime factors including only odd square-free prime factors of the odd number n and sufficiently so large integers or all of prime factors values tend to infinity versus the number of them, then the equation

$$n - m \prod_{p_i \leq p \leq p_k} (p - 1) = \pm 1 \quad (2.4)$$

does not any solution. m denotes a positive integer.

2.5. Theorem 4:

Let p_1 to p_k be all of the prime factors including only odd square-free prime factors of the odd number n , all of them be existed, and p_k sufficiently so large integer or tends to infinity, then the equation

$$n - m \prod_{p \leq p_k} (p - 1) = \pm 1 \quad (2.5)$$

does not any solution. m denotes a positive integer.

2.6. Theorem 5:

Let p_i to p_k be all of the prime factors including only odd square-free prime factors of the odd number n and p_k sufficiently so large integer or tends to infinity, then

$$n - m \prod_{p_i \leq p \leq p_k} (p - 1) = \pm 1 \quad (2.6)$$

does not any solution. m denotes a positive integer.

2.7. **Theorem 6:**

Let p_i to p_k be all of the prime factors including only odd square-free prime factors of the odd number n , and none of them be so large and unbounded (all of them be bounded), then the equation

$$n - m \prod_{p_i \leq p \leq p_k} (p - 1) = 1 \quad (2.7)$$

does not any solution, but the equation

$$n - m \prod_{p_i \leq p \leq p_k} (p - 1) = -1 \quad (2.8)$$

may have solutions. m denotes a positive integer.

3. Proofs

3.1. **Proof of Theorem 1**

As is well-known, Mertens himself has proven this theorem but we give another method for making its proof. We really reprove (reformulate) the proof. The proof can be made by applying three times *the Abel summation formula* to the the series

$$\sum_{p \leq x} \frac{1}{p} = \sum_{p \leq x} \frac{\log p}{p} \cdot \frac{1}{\log p} \quad (3.1)$$

Firstly, we apply it to the series $\sum_{p \leq x} \log p$ and reach to $\theta(x) = x + o(\frac{x}{\log x})$. Secondly, $\sum_{p \leq x} \frac{\log p}{p}$. Let $\sum_{p \leq x} \log p = \theta(x)$ and $\phi(x) = \frac{1}{x}$ and substitute them into the Abel summation formula as follows:

$$\sum_{p \leq x} \frac{\log p}{p} = \theta(x)\phi(x) + \int_1^x \frac{\theta(u)}{u^2} du \quad (3.2)$$

Then, we have

$$\sum_{p \leq x} \frac{\log p}{p} = 1 + \log(x) + o(\log \log x) \quad (3.3)$$

Thirdly, we apply it to the entire series. Let $A(x) = \sum_{p \leq x} \frac{\log p}{p}$ and $\Phi(x) = \frac{1}{\log(x)}$ into the Abel summation formula

$$\begin{aligned} \sum_{p \leq x} \frac{1}{p} &= A(x)\Phi(x) + \int_2^x A(u) \cdot \Phi'(u) \cdot du = \{1 + \log x + o(\log \log x)\} \cdot \left(\frac{1}{\log x}\right) \\ &+ \int_2^x \frac{\{1 + \log u + o(\log \log u)\}}{u(\log u)^2} du = 1 + \log x + o\left(\frac{\log \log x}{\log x}\right) + \int_2^x \frac{du}{u(\log u)^2} + \\ &\int_2^x \frac{du}{u \log u} + \int_2^x o\left(\frac{\log \log u}{u(\log u)^2}\right) = 1 + \frac{1}{\log 2} - \log \log 2 + \log \log x + o\left(\frac{\log \log x}{\log x}\right) + d + \\ &o\left(\frac{\log \log x}{\log x} + \frac{1}{\log x}\right) = 1 + \frac{1}{\log 2} - \log \log 2 + d + \log \log x + o\left(\frac{1}{\log x}\right) \end{aligned} \quad (3.4)$$

Where d denotes all unknown constant values created in (3.4). Since according to the properties of small "o" and big "O" notations, we have $o(\frac{1}{\log x}) = O(\frac{1}{\log x})$, then

$$\sum_{p \leq x} \frac{1}{p} = \log \log x + a + O\left(\frac{1}{\log x}\right) \quad (3.5)$$

where $a = 1 + \frac{1}{\log 2} - \log \log 2 + d$. Although, precisely calculating a is difficult, but our attempts to calculate the value a using directly processing data by substituting into (3.5) gave us an approximate value about 0.261497...

3.2. *Proof of Theorem 2*

The proof can be found in the Mertens' paper [6].

3.3. Proof of Corollary 1

The proof can easily be made by appealing to the Riemann Zeta Function and Euler's product [7] as follows:

$$\zeta^{-1}(s) = \prod_p \left(1 - \frac{1}{p^s}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} \quad (3.6)$$

Putting $s = 1$ in (3.6), we have

$$\prod_p \left(1 - \frac{1}{p}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \quad (3.7)$$

and trivially checking gives us

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) > \prod_p \left(1 - \frac{1}{p}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} \quad (3.8)$$

Abel Summation Formula gives us again that assuming $\sum_{n \leq x} \mu(n) = o(x)$ [7], we have

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = \frac{e^{-\gamma}}{\log x} + o(\log(x)) \quad (3.9)$$

Combining (3.9) with theorem 2 and (3.8) we find

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) > \prod_p \left(1 - \frac{1}{p}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} = \frac{e^{-\gamma}}{\log x} + o(\log(x)) > \frac{c}{\log(x)} \quad (3.10)$$

If we let $c < e^{-\gamma}$, then inequality and the theorem is completed. We choose $c = 0.3$ in this paper. On the other hand, we appeal to Theorem 7, Corollary of the Rosser and Schoenfeld's paper [8] (the relation (3.27)) and we find that for $x = 3$, we can choose $c = 0.09$ since the term $e^{-\gamma}(1 - \frac{1}{(\log 3)^2}) = 0.0962709\dots$. Therefore, we choose a new lower bound for c i.e. $c = 0.09$ since we have $e^{-\gamma}(1 - \frac{1}{(\log x)^2}) > e^{-\gamma}(1 - \frac{1}{(\log 3)^2}) > 0.09$ for all the odd primes ≥ 3 . Also, Dusart [9] in 2010, stated the Theorem 6.12 giving a new bound for all $x \geq 2973$. This new bound for $x \geq 2973$ is $0.46842432\dots$. This means that $c = 0.3$ is acceptable for these values as well.

3.4. *Proof of Theorem 3*

If we divide both of sides of the equation (2.4) by $\prod_{p_i \leq p \leq p_k} (p-1)$, then

$$\frac{1}{\prod_{p_i \leq p \leq p_k} (1 - \frac{1}{p})} - m = \frac{\pm 1}{\prod_{p_i \leq p \leq p_k} (p-1)} \quad (3.11)$$

Since $n = p_i \dots p_k$ is odd and p_i to p_k are also odd square-free prime factors of n , then trivially all of them must be ≥ 3 and follows $\frac{1}{\prod_{p_i \leq p \leq p_k} (p-1)} < \frac{1}{8}$ if the numerator of right side be $(+1)$ and $-\frac{1}{\prod_{p_i \leq p \leq p_k} (p-1)} > -\frac{1}{8}$ if the numerator of right side be (-1) . On the other hand, the left side of (3.11) should be greater than zero for the plus sign and less than zero for the minus sign. Therefore, for plus sign we have

$$\frac{1}{\prod_{p_i \leq p \leq p_k} (1 - \frac{1}{p})} - \frac{1}{8} < m < \frac{1}{\prod_{p_i \leq p \leq p_k} (1 - \frac{1}{p})} \quad (3.12)$$

and for minus sign

$$\frac{1}{\prod_{p_i \leq p \leq p_k} (1 - \frac{1}{p})} < m < \frac{1}{\prod_{p_i \leq p \leq p_k} (1 - \frac{1}{p})} + \frac{1}{8} \quad (3.13)$$

Since our assumption says us that all p_i to p_k tend to infinity versus the number of primes within the interval (p_i, p_k) , the relations (3.12) and (3.13) change to

$$1 + \varepsilon - \frac{1}{8} < m < 1 + \varepsilon \quad (3.14)$$

$$1 + \varepsilon < m < 1 + \varepsilon + \frac{1}{8} \quad (3.15)$$

when ε tends to zero. This is due to if we let M denotes the number of primes from p_i to p_k (note: there may not exist all of consecutive primes within the interval (p_i, p_k)) then we find

$$(1 - \frac{1}{p_i})^M \leq \prod_{p_i \leq p \leq p_k} (1 - \frac{1}{p}) \leq (1 - \frac{1}{p_k})^M \quad (3.16)$$

Since according to our assumption, p_i to p_k are so large versus M , then all the fractions $\frac{M}{p_i}$ to $\frac{M}{p_k}$ tend to zero and

$$\lim_{p_i \rightarrow \infty} (1 - \frac{1}{p_i})^M = \lim_{p_i \rightarrow \infty} \{(1 - \frac{1}{p_i})^{p_i}\}^{\frac{M}{p_i}} = \lim_{p_i \rightarrow \infty} (\frac{1}{e})^{\frac{M}{p_i}} = 1 \quad (3.17)$$

and in the similar way

$$\lim_{p_k \rightarrow \infty} (1 - \frac{1}{p_k})^M = 1 \quad (3.18)$$

Then the inequality (3.16) gives us

$$\lim_{p_i \text{ to } p_k \rightarrow \infty} \prod_{p_i \leq p \leq p_k} (1 - \frac{1}{p}) = 1 \quad (3.19)$$

This means that the integer number m can only be 1 when (3.14) holds and cannot be any integer number when (3.15) holds. If $m = 1$, it is impossible to hold by appealing to Lehmer's paper [1] since $m = 1$ if and only if n is prime. This completes the proof.

3.5. *Proof of Theorem 4*

If we divide both of sides of (2.5) by $n = p_1 \dots p_k$ and substitute $\prod_p (1 - \frac{1}{p}) = \frac{e^{-\gamma}}{\log x} + o(\log(x))$ from (3.8) and (3.9) into it, then let $x = p_k$

$$1 - m \left\{ \frac{e^{-\gamma}}{\log p_k} + o(\log(x)) \right\} = \frac{\pm 1}{p_1 \dots p_k} \quad (3.20)$$

Since $p_k \rightarrow \infty$ then also $x \rightarrow \infty$ and (3.20) changes to

$$1 - \frac{m}{e^{\gamma} \log p_k} = \frac{\pm 1}{p_1 \dots p_k} \quad (3.21)$$

The right side tends to zero since $p_k \rightarrow \infty$. This means that the left side should also tend to zero and m is of order $e^{\gamma} \log x$. Since m is a positive integer, it could be of the form

$$m = [e^{\gamma} \log p_k] = e^{\gamma} \log p_k - \alpha \quad (3.22)$$

for plus sign since the left side of (3.21) should be closed to 0^+ or

$$m = [e^\gamma \log p_k] + j = e^\gamma \log p_k + j - \alpha \quad (3.23)$$

for minus sign since the left side of (3.21) should be closed to 0^- where $j \geq 1$ and denotes an integer, the sign $[]$ denotes the integer part of a number, and α denotes the fractional part of $e^\gamma \log x$. Therefore, the relation (3.21) can be changed into

$$\frac{\alpha}{e^\gamma \log p_k} = \frac{1}{p_1 \dots p_k} \quad \text{or} \quad \frac{j - \alpha}{e^\gamma \log p_k} = \frac{1}{p_1 \dots p_k} \quad (3.24)$$

for when $p_k, x \rightarrow \infty$. Since the denominator of the right side fraction of (3.24) is of the order more than p_k and the denominator of the left right fraction is of order $\log p_k$, α and $j - \alpha$ are also bounded, then these two sides cannot be equal for when p_k is tending to infinity and the equation (3.24), (3.21), and finally (2.5) cannot have any solutions.

3.6. *Proof of Theorem 5*

The proof of this theorem also likes to Theorem 4. Consider all primes p_i to p_k exist or missing some of them, then regarding Theorem 2

$$A(p) \cdot \prod_{p_i \leq p \leq p_k, p_k \rightarrow \infty} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log p_k} \quad (3.25)$$

where $A(p)$ denotes a function of prime numbers before p_k or some before p_k and some between p_i and p_k for completing and converting $\prod_{p_i \leq p \leq p_k} (1 - \frac{1}{p})$ to $\prod_{p \leq p_k} (1 - \frac{1}{p})$, which may be a constant value or variative one. Similarly to (3.21), we have

$$1 - \frac{m}{A(p)e^\gamma \log p_k} = \frac{\pm 1}{p_1 \dots p_k} \quad (3.26)$$

where

$$A(p) = \prod_{p \leq p_{(i-1)}} \left(1 - \frac{1}{p}\right) \text{ or } A(p) = \prod_{p \leq p_{(i-1)}} \left(1 - \frac{1}{p}\right) \cdot \prod_{p_i \leq p_m \leq p_k} \left(1 - \frac{1}{p_m}\right) \quad (3.27)$$

and p_m denotes primes missing within the interval (p_i, p_k) . Trivially, $A(p) <$

1. Similarly to the proof of Theorem 4, we find

$$m = [A(p)e^\gamma \log p_k] = A(p)e^\gamma \log p_k - \beta \quad (3.28)$$

for plus sign since the left side of (3.26) should be closed to 0^+ or

$$m = [A(p)e^\gamma \log p_k] + j = A(p)e^\gamma \log p_k + j - \beta \quad (3.29)$$

since the left side should be closed to 0^- for when $p_k \rightarrow \infty$. Therefore,

(3.26) changes to

$$\frac{\beta}{A(p)e^\gamma \log p_k} = \frac{1}{p_1 \dots p_k} \quad (3.30)$$

or

$$\frac{j - \beta}{A(p)e^\gamma \log p_k} = \frac{1}{p_1 \dots p_k} \quad (3.31)$$

Where $0 \leq \beta < 1$. To being better closed to zero in relation (3.31), we should choose $j = 1$. The arguments are similar to the arguments of Theorem 4 and the proof is completed.

3.7. **Proof of Theorem 6**

Regarding Corollary 1, we have

$$\frac{c}{\log p_k} < \prod_{p \leq p_k} \left(1 - \frac{1}{p}\right) = \prod_{p_1 \leq p \leq p_{(i-1)}} \left(1 - \frac{1}{p}\right) \cdot \prod_{p_i \leq p_m \leq p_k} \left(1 - \frac{1}{p_m}\right) \cdot \prod_{p_i \leq p \leq p_k} \left(1 - \frac{1}{p}\right) \quad (3.32)$$

where p_m denotes primes missing within the interval (p_i, p_k) . Let $A(p) = \prod_{p_1 \leq p \leq p_{(i-1)}} (1 - \frac{1}{p}) \cdot \prod_{p_i \leq p \leq p_k} (1 - \frac{1}{p_m})$ and knowing $A(p) < 1$ then

$$\frac{c}{A(p) \log p_k} < \prod_{p_i \leq p \leq p_k} (1 - \frac{1}{p}) \quad (3.33)$$

and multiplying the left side by a coefficient $l_k > 1$, we find an equation

$$\frac{cl_k}{A(p) \log p_k} = \prod_{p_i \leq p \leq p_k} (1 - \frac{1}{p}) \quad (3.34)$$

Similarly to (3.26), we have

$$1 - \frac{mcl_k}{A(p) \log p_k} = \frac{\pm 1}{p_i \dots p_k} \quad (3.35)$$

As the Theorems 4 and 5 arguments, we have

$$m = [A(p) \frac{\log p_k}{cl_k}] = \frac{A(p) \log p_k}{cl_k} - \psi \quad (3.36)$$

for plus sign since the left side of (3.35) should be closed to 0^+ or

$$m = [A(p) \frac{\log p_k}{cl_k}] + j = \frac{A(p) \log p_k}{cl_k} + j - \psi \quad (3.37)$$

for minus sign to be closed to 0^- (According to Lehmer's, Cohen's, Kishore's, and Lieuwen's arguments, the number of prime numbers to have a composite solution should be more than 7,14,33, or 212. Thus, the value $\frac{1}{p_i \dots p_k}$ should be certainly closed to zero due to being large the value $p_i \dots p_k$). $0 \leq \psi < 1$ denotes the fractional part of a positive real number. Therefore, the equations (2.7) and (2.8) are found respectively

$$\frac{\psi cl_k}{A(p) \log p_k} = \frac{1}{p_i \dots p_k} \quad (3.38)$$

and

$$\frac{(j - \psi) cl_k}{A(p) \log p_k} = \frac{1}{p_i \dots p_k} \quad (3.39)$$

As we know, $\log p_k$ isn't an integer number and since $cl_k > 0.09$ regarding Corollary 1 and $A(p)$ tends to zero by increasing the number of primes and being larger $p_{(i-1)}$ and p_k , then the value $\frac{A(p)}{cl_k}$ gets smaller and smaller and $\log p_k$ larger and larger, thus the fractional part of $A(p)\frac{\log p_k}{cl_k}$ gets closer to the number 1. This means that ψ gets closer to the number 1 to that of zero. Therefore, since $\frac{\psi cl_k}{A(p)}$ gets larger than 1, then (3.38) cannot have any solution, but may (3.39) have solution since $(j - \psi)$ gets closer to zero with $j = 1$ and $\frac{(1-\psi)cl_k}{A(p)}$ gets closer to zero as well. As Lehmer [1], Kishore [4], Cohen [5], and specifically Lieuws [3] showed that if the case $n - m \prod_{p_i \leq p \leq p_k} (p - 1) = 1$ has composite solution, then the number of prime factors should be at least 7, 14, 33 or 212, therefore, we see that the order of magnitude of n must be very large and our hypothesis can be more precise.

Example:

Lehmer showed that $n = 3.5.17.257$ is a composite solution for the equation $n - m \prod_{p_i \leq p \leq p_k} (p - 1) = -1$. We compute the values $1 - \psi$, $A(p)$, cl_k , and $\log p_k$ assuming $c = 0.09$ and substitute them into (3.38) and (3.39) as follows:

Here, we have $p_i = 3$, $p_{i+1} = 5$, $p_{i+5} = 17$, $p_k = 257$. For computing $A(p)$, one should compute all of other missing primes as:

$$\begin{aligned} A(p) &= (1 - \frac{1}{7})(1 - \frac{1}{11})(1 - \frac{1}{13})(1 - \frac{1}{19})(1 - \frac{1}{23}) \dots \\ &(1 - \frac{1}{211})(1 - \frac{1}{223})(1 - \frac{1}{227})(1 - \frac{1}{229})(1 - \frac{1}{233}) \\ &(1 - \frac{1}{239})(1 - \frac{1}{241})(1 - \frac{1}{251}) = 0.39984516 \end{aligned} \quad (3.40)$$

The relation (3.34) gives us $\prod_{p_i \leq p \leq p_k} (1 - \frac{1}{p}) = 0.50000763$, $\log p_k = \log 257 = 5.54907608$, $l_k = 12.3266964$, and $\psi = 0.99996922$. Just, we are ready to

compute the left sides of the two relations (3.38) and (3.39).

From the left side of the relation (3.38), we find

$$\frac{\psi cl_k}{A(p) \log p_k} = 0.49999238 \quad (3.41)$$

and from the left side of (3.39) with $j = 1$ we find

$$\frac{(1 - \psi) cl_k}{A(p) \log p_k} = 1.526023 \times 10^{-5} \quad (3.42)$$

If we compute the right side of each of two relations (3.38) and (3.39)

$$\frac{1}{p_i \dots p_k} = \frac{1}{3 \times 5 \times 17 \times 257} = 1.525902 \times 10^{-5} \quad (3.43)$$

and compare to the corresponding left sides (the relations (3.41) and (3.42)), then we find that the equation (2.8) has a solution since the left and right sides are very close to each other, but the equation (2.7) (same Lehmer's conjecture) does not any solution since the left and right sides are far from each other. Another example can be made by other composite number $n = 3.5.17.257.65537$, which Lehmer showed it can be a composite solution for the same equation. Since $p_k = 65537 \geq 2973$, we consider $c = 0.3$ for our calculations.

3.8. *Lehmer's totient conjecture*

We discuss about Lehmer's totient conjecture here. Firstly, we know if n is a prime number p , then $\phi(n) = p - 1$ and trivially implies $n - 1 \equiv 0 \pmod{\phi(n)}$. Conversely, if we have $n - 1 \equiv 0 \pmod{\phi(n)}$, then let $n = p_1^{t_1} \dots p_k^{t_k}$ be prime factors decomposition of n . This means that $\phi(n) = p_1^{t_1} \dots p_k^{t_k} \prod_{p_1 \leq p \leq p_k} (1 - \frac{1}{p})$. If $t_1, \dots, t_k \geq 2$, then we find that $p_1, \dots, p_k | \text{both } \phi(n) \text{ and } n$. On the other hand, regarding our assumption $n - 1 \equiv 0 \pmod{\phi(n)}$ and we

should have $p_1, \dots, p_k | (n-1)$. But, these imply that $p_1, \dots, p_k | \gcd(n, n-1) = 1$, which is impossible to occur. Hence, n can have neither square prime factors nor can be an even number (this is a Lehmer's theorem, which we prove it here by other method). This means that $t_1 \dots t_k \leq 1$, thus some of t_1, \dots, t_k must be 0 or 1 or all of them be 1. Also, all of prime factors must be odd numbers. Certainly, if all of t_1, \dots, t_k be zero but one, then $n = p$ and the problem is solved. If the number of square-free prime factors are greater than or equal 2, then using Theorems 3 to 6 of this paper, we find out the equation

$$n - m \prod_{p_i \leq p \leq p_k} (p - 1) = 1 \quad (3.44)$$

does not any solution and Lehmer's totient conjecture is proven.

Acknowledgment

This paper was submitted to a journal and quickly took some comments for its amendment. The author would like to thank anonymous referee for his/her nice comments. Also, thanks for Mr. Alexander Zujev, research scholar, University of California at Davis for his interesting comments on the paper. All the needed comments have been taken into account to the paper.

References

- [1] D.H. Lehmer, On Euler's totient function, Bull. Amer. Math. Soc. 38(1932), 745-751.
- [2] R. G. E. Pinch, A note on Lehmer's totient problem, personal web site, (2006) p.1.

- [3] E. Liewens, Do there exist composite numbers for which $k\phi(M) = M - 1$ holds?, Nieuw. Arch. Wisk.18 (1970), 165-169.
- [4] M. Kishore, On the number of distinct prime factors of n for which $\phi(n)|(n - 1)$,Nieuw. Arch. Wisk.25 (1977), 48-53.
- [5] G.L. Cohen and P.Hagis jr., On the number of prime factors of n if $\phi(n)|(n - 1)$,Nieuw. Arch. Wiskd.,III. Ser. 28 (1980), 177-185.
- [6] F. Mertens, Ein beitrage zur analytischen zahlentheorie, J.reine angew. Math. 78 (1874), 46-62.
- [7] William and Fern Ellison,*Prime Numbers*, Wiley-Interscience,a division of John Wiley and Sons.Inc.New York (1985).
- [8] J.B. Rosser, L.Schoenfeld,Approximate formulas for some functions of prime numbers, Illinois J.Math.**6** (1962) 64-94
- [9] P. Dusart, Estimates of some functions over primes without R.H., arXiv:1002.0442v1, Feb. 2,2010